



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,914	12/10/1999	GERMANO CARONNI	06502.0289	8208

22852 7590 12/13/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

HA, LEYNNA A

ART UNIT PAPER NUMBER

2135

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/457,914

Applicant(s)

CARONNI ET AL.

Examiner

LEYNNA T. HA

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 September 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39 and 41-48 is/are pending in the application.
- 4a) Of the above claim(s) 4, 6, 12, 21, 23, 32, 38 and 40 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39 and 41-48 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4/8/005 & 4/14/05 11/2/05

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 22, 2005 has been entered.

2. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 have been considered and are pending.

Applicant have amended independent claims 1, 16, 18, 29, 33, and 35.

Cancelled claims are 4, 6, 12, 21, 23, 32, 38, and 40.

3. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 remains rejected under 35 U.S.C. 112, 1st paragraph.

4. *Claim Rejections - 35 USC § 112*

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

In the last (Final) office action, claims 1, 16, 18, 29, 33, and 35 were rejected as containing new matter issues wherein the specification fails to support "without passing through the private network" as amended by Applicant. The independent claims is currently amended to include the "administrative machine" and deleted the "private network" whereby the limitation "without passing through" remains. The examiner agrees that the "administrative machine" is taught in the specification, but as indicated before the limitation "without passing through" was not disclosed in the specification. Even though

Art Unit: 2135

the administrative machine is taught, the limitation of “without passing through the administrative machine” as an entirety is not disclosed nor explained in the specification.

Applicant have responded pointing to pages 8-12 of the specification, indicating that this limitation was disclosed. According to page 9 on line 10, the specification merely mention once that the Supernet also includes an administrative node, but fails to explain further that transmitting a packet “without passing through the administrative machine”. In addition, on page 12 starting on line 15 and continues onto page 16, describes the administrative machine as including functions such as authenticating nodes (pg.13, lines 11-12), key management and may act as a server (pg.14, lines 3-5, 19-20), and performs security functionality as well as address translation (pg.16, lines 3-17). Nowhere on these pages that goes into details explaining the administrative machine indicate “without passing through the administrative machine”.

Specification explains the Supernet node is part of the Supernet which includes an administrative machine (as discussed above) wherein the component (i.e. a security layer in a protocol stack) enforces all communications to and from this node travel through the security infrastructure of the Supernet so that this node can communicate with other members of the Supernet and non-members of the Supernet cannot access this node (pg.12, lines 6-10). In addition, claim language discloses the administrative machine verifies node identification and sending security context information which indicates the administrative machine performs security functions prior to transmitting a packet. The administrative

Art Unit: 2135

machine as claimed and in the specification implies the same functions. Hence, specification confirms that communications must pass through the security infrastructure which is the administrative machine of the Supernet. Thus, specification and some of the claim language contradicts to the amended limitation of transmitting the packet "without passing through the administrative machine". Therefore, verifies that this limitation is new subject matter being introduced and will not be entered or considered for the rejection.

All other claims are also rejected due to their dependencies.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Devine, et al. (US 6,606,708).

Applicant is noted that the new matter limitations of “without passing through the administrative machine” have not been entered for consideration.

As per claims 1, 18, and 35:

Devine, et al. teaches a method executed in a data processing system for providing communication access between a first process associated with a first node and a second process associated with a second node, the method comprising:

sending a request from the first node (col.8, lines 23-30 and col.13, lines 31-33) to an administrative machine (col.10, lines 55-59 and col.23, lines 17) to verify a first node identification associated with the first process; (col.8, lines 30-32 and 61-67)

Art Unit: 2135

in response to the request, receiving security context information at the first node from the administrative machine, the security context information comprising a virtual address for the first node; **(col.13, lines 45-51 and col.24, lines 8-9)**

appending the security context information for the first process in a process table; **(col.9, lines 60-63, col.13, lines 60-67)**

opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

transmitting a packet from the first process to the second process through the open socket **(col.26, lines 54-57)**, the packet comprising the security context information for the first process in the process table **(col.14, lines 6-11)**.

As per claims 2, 19, and 36: See **col.12, lines 34-37**; discusses modifying a socket structure so as to accept the security context information.

As per claims 3, 20, and 37:

Devine discloses receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

Art Unit: 2135

As per claims 5, 22, and 39: See col.27, line 43 thru col.28, line 5; discusses comparing the security context information in the received packet and security context information in another process table.

As per claims 7, 24, and 41: See col.20, lines 53-63 and col.22, lines 25-30; discusses determining whether the first and second process belong to two different linked channels ; and permitting use of the packet when the different channels are linked. (col.23, lines 7-11)

As per claims 8, 25, and 42: See col.24, line 2 and col.26, lines 40-42; discusses determining whether the first and second process belong to two different linked channels includes initiating a process that spawns two child processes that are connected by a shared-memory region in a memory.

As per claims 9, 26 and 43: See col.8, lines 27-28 and col.12, lines 34--37; discusses permitting use of the packet includes decrypting the packet on a node and authenticating a sender associated with the first process on the node.

As per claims 10 and 27: See col.9, lines 2-10 and col.14, lines 6-11; discusses obtaining the security context information from a third process, the security context information comprising a virtual address and a node identification.

As per claims 11, 28 and 45: See col.13, lines 31-67; discusses modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit.

Art Unit: 2135

As per claim 13: See col.8, lines 52-55; discusses receiving a key that corresponds to the first node identification from the server.

As per claim 14: See col.9, lines 6-13 and col.13, lines 31-67; discusses encrypting a packet transmitted by the first process using the key; and encapsulating the encrypted packet with a header that comprises the first node identification.

As per claim 15:

Devine teaches a method of claim 1, further comprising:

 sending a second request from the second node (col.14, lines 6-35) to the server to verify node identification; (col.13, lines 65-67)

 receiving additional security context information comprises from the server, wherein the additional security context information includes a second virtual address for the second node; (col.22, lines 25-30 and col.23, lines 26-28)

 creating the second process; and appending the security context information for the second process in the process table associated with the second process. (col.14, lines 23-30 and col.24, lines 8-14)

As per claims 16 and 33:

Devine teaches a method executed in a data processing system for providing secure communications between a first process associated with a first node and a second process associated with a second node, comprising:

 obtaining node identification comprising a virtual address from an administrative machine; (col.10, lines 55-59 and col.23, lines 17)

Art Unit: 2135

including the node identification in a field corresponding to the first process in a process table; **(col.13, line 65 thru col.14, line 2)**

transmitting a datagram that contains the node identification the first process to a socket; and **(col.13, lines 60-63)**

receiving the datagram at the second process that contains the node identification and a second virtual address **(col.22, lines 55-56 and col.23, lines 26-28).**

As per claims 17 and 34:

Devine teaches the method of claim 16, wherein obtaining a node identification further comprises:

modifying a socket structure in the socket so that the socket structure accepts the node identification; and **(col.13, lines 31-67)**

modifying a process table so that the table comprises a node identification field. **(col.23, lines 26-31 and col.26, lines 24-31)**

As per claim 29:

Devine teaches a system for placing a process executed in a node in a security context, comprising:

an administrative machine; and **(col.6, line 8-9)**

a sending node comprising:

a transmission module that transmit a request an administrative machine **(col.10, lines 55-59 and col.23, lines 17)** to verify a sending node identification **(col.8, lines 30-32 and 61-67)**, and receives security context information from the administrative machine in response to the request, wherein the security

Art Unit: 2135

context information comprises a virtual address for the sending node; **(col.13, lines 45-51 and col.24, lines 8-9)**

memory containing a process and an associated process table; and **(col.9, lines 60-63, col.13, lines 60-67)**

an appending module that appends the received security context information **(col.9, lines 60-63, col.13, lines 60-67)** and the sending node identification for the process in the process table **(col.13, line 43 thru col.14, line 17)**, wherein the transmission module transmits a packet from the process to a receiving node **(col.26, lines 54-57)**, the packet comprising the security context information for the first process in the process table. **(col.14, lines 6-11)**

As per claim 30: See col.8, lines 52-55; discusses the transmission module further receives a key that corresponds to the sending node identification from the administrative machine.

As per claim 31: See col.9, lines 6-13 and col.13, lines 31-67; discussing an encryption module that encrypts the packet transmitted by the process using the key; and an encapsulating module that encapsulates the encrypted packet with a header that comprises the sending node identification.

Art Unit: 2135

As per claim 44:

Devine teaches the computer readable medium of claim 35, wherein the appending module comprises:

an obtaining module for obtaining the security context information from a third process, the security context comprising a virtual address and a node identification; and **(col.9, lines 2-10 and col.23, lines 61-64)**

a limiting module for limiting each of the first, second and third processes to communicate with another process provided that the communicating processes share the same node identification. **(col.9, lines 2-10 and col.22, lines 25-30)**

As per claim 46: See col.8, lines 31-32 and 14, lines 23-30; discusses determining if the first and second process belong to a channel; and accepting the transmitted packet when the first and second process belong to the channel.

As per claim 47: See col.8, lines 31-32 and 14, lines 23-30; discusses means for determining if the first and second process belong to a channel; and means for accepting the transmitted packet when the first and second process belong to the channel.

As per claim 48: See col.8, lines 31-32 and 14, lines 23-30; discusses determining module for determining if the first and second process belong to a channel; and an accepting module for accepting the transmitted packet when the first and second process belong to the channel.

Response to Arguments

The first node is in the form of client workstation 10 wherein the request is initiated at the client browser to verify the session for that particular workstation (col.10, lines 39-40). Session is in the form of applicant's process because like the process, the session relates to the communicative entity of a client's node or workstation. The DMZ acts as a double firewall that includes DMZ server 24 which is in the form of an administrative machine where the server 24 is a system or an equipment that provides secure messaging session or process (col.10, lines 2-4 and 13-14) and forwards over a secure socket connection to the second session associated to a second node which is the dispatcher server 25 (col.8, lines 33-35). The server 24 prevent potentially hostile customer access wherein verifying if the request is from a valid user by the user's information contained in a message and after establishing the user is valid, the request is mapped to it associated session (col.13, lines 60-62). Devine describes one of the process of verifying the user consist of session data/cookie mapping where the server generates a cookie or session identifier where the client holds on to the cookie so that the client can return it for subsequent request to the server 24 to identify the client and to map to the associated session (col.8, lines 62-58) and uses virtual IP addressing. Devine explains the server send to the client security information within the DMZ web header of the cookie which consist of transaction type identifier, target proxy identifier

Art Unit: 2135

associated with the particular type of transaction requested and proxy specific data (col.13, lines 46-51).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa



KIM VU
PATENT EXAMINER
EBC CENTER 2135